Notice of Allowability	Application No.	Applicant(s)	
	09/202,024	SCHAEFER-LORINSER ET AL.	
	Examiner	Art Unit	
	FIRMN BACKER	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *November 14th, 2005*.

2. ☒ The allowed claim(s) is/are *15-29*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

FIRMIN BACKER
PRIMARY EXAMINER

Response to Request for Reconsideration

This is in response to a request for reconsideration file November 14th, 2005. Claims 15-29 are being reconsidered in this action.

Response to Arguments

1. Applicant's arguments filed November 14th, 2005 have been fully considered and they are persuasive.

Allowable Subject Matter

2. Claims 15-29 are allowed over the prior arts.

3. The following is an examiner's statement of reasons for allowance:

a. Applicant discloses a method for loading input data into a program when performing a cash transaction between a cash chip and a security module. Applicant's disclosure is novel and innovative in the sense in claims 15 it loads data blocks into a linear feedback register having shift register non-linear function cryptographically enhances using a downstream counter and introducing an additional feedback into the linear feedback shift register following the downstream counter and switching off one additional feedback after a pre-defined first number of pulses of an associated clock. Furthermore in claim 24, the invention provides one additional nonlinear feedback shift register for cryptographically enhancing the circuit and being connected to the circuit and

one additional non-linear feedback shift register disconnectable. The closet prior art Taylor discloses a method that provides a digital data stream generator for generating a cipher stream comprising a linear feedback shih register (LFSR), a summing means for producing a sequence of sums of the outputs of said at least one LFSR, a non-linear feedback processing means for producing a sequence of non-linear values in accordance with the outputs of said at least one LFSR and at least one previous value of said non-linear output value sequence, and an output processing means for generating a data stream in accordance with a Bent function utilizing a plurality of pairs of said sequence of sums and at least one of said sequence of non-linear values. Taylor fail to teach the invention disclose in claims 15 and 24.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Koopman et al (US RE36181) teach an invention, wherein cryptographic authentication of transmissions from a remote transmitter to a receiver module involves encryption, such as by linear feedback shift register pseudorandom number generation

operations, utilizing secret feedback masks which are essentially unique to each transmitter, and replicated only in a receiver which is to respond to the related transmitter.

b. *Muller et al (WO 01/15090) teach a shift register with linear and non-linear feedback functions for creating cryptographic algorithms. The cryptographic algorithms are provided for enciphering data and authenticating the card against deriving the secret key used from statistical analysis of information leaking away to outside world in the event of cryptographic operations.*

c. *Matsumoto (NPL) teach a chip containing a "mixture generator," three linear feedback registers that simultaneously run data-encrypting calculations and spew out the encrypted data.*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FIRMN BACKER whose telephone number is 571-272-6703. The examiner can normally be reached on Monday - Thursday 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (571) 272-6712. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

FIRMN BACKER
Primary Examiner
Art Unit 3621

January 3, 2006